Classification des injections virtuelles

Christophe Chalons

Classification des injections virtuelles

Christophe Chalons, Paris7

3 novembre 2014

1 Introduction

Les auteurs ayant contribué et construit cette version2 sont :

Anatole Khélif, Saab Abou Jaoudé, Francis Jamet, et Christophe C

Dans la suite de l'article on classe les injections virtuelles d'un entier dans un autre telles que définies dans :

Christophe Chalons. Le paradigme téléphonique. Logic. IMJ Paris 7, 2014. French. <tel-01076047> ; lien internet : https ://hal.archives-ouvertes.fr/tel-01076047

article qui pour être mieux compris peut être complété par la lecture de :

Christophe Chalons. Cadre logique pour les degrés ludiques. Formalisation d'une question réputée informalisable. 2014. <hal-01056193> ; lien internet : https ://hal.archives-ouvertes.fr/hal-01056193v1

Le théorème a été démontré dans un premier temps par Anatole Khélif. Si $p = qp' + r$ et $r < p'$ alors

$$[(n,p) \leq (n',p') \iff n \leq qn' + r]$$

Afin que cette introduction soit self-contained, on donne la définition à froid (le corps de l'article précisant les choses avec plus d'affection) de $(n,p) \leq (n',p')$: c'est une abréviation pour dire *il existe des applications* f,g,h,k *allant respectivement de* $n \to n'$ *;* $n \times p' \to p$ *;* $p \to p'$ *et* $p \times n' \to n$ *vérifiant*

$$\forall x,y : [k(g(x,y),f(x)) = x \text{ et } (\exists t : x \neq k(g(x,y),t)) \Rightarrow y = h(g(x,y))]$$

La démonstration d'Anatole (de la condition nécessaire) était en deux parties un peu mystérieuses :

En regardant l'ensemble $A := \{x \in n \mid \forall y \in p' \exists t \in n' : x \neq k(g(x,y),t)\}$ et en remarquant que $(x,y) \mapsto (g(x,y),f(x))$ est injective de $A \times p'$ dans $p \times n'$, si on note a la cardinal de A, il n'était pas très dur de voir, en dénombrant un grand nombre de $g(x,y)$ différents les uns des autres dans p, les uns choisis tels que $x \in A$ les autres choisis tels que $x \notin A$, qu'on a forcément

$$[a/n'] \times p' + n \leq p + a$$

.

En se livrant à l'exercice suivant : pour tout $x \in \{0; \dots n\}$, si $[x/n'] \times p' + n \leq p + x$ alors $n \leq qn' + r$

Par la suite Francis Jamet et Saab Abou Jaoudé ont revisité le phénomène et grâce à deux lemmes de Francis Jamet, Abou a pu construire une démonstration tout en douceur que la suite de l'article révèle. Les points clés ont été d'étudier les images réciproques par g des singletons qui sont forcément des lignes ou des colonnes de $n \times p'$ et finalement de mieux sentir les propriétés de la fonction g à la fois pour elle-même et pour obtenir d'une autre manière la CN.

La caractère suffisant de la CNS est, elle, triviale quand on s'est un peu familiarisé avec le paradigme téléphonique et résulte de :

$$(n,p) \leq (kn,kp) \leq (kn+1,kp+1) \leq (kn+2,kp+2) \leq (kn+3,kp+3) \leq etc, etc$$

La toute dernière section donne la preuve d'Anatole. **Toutes les sections à partir de la suivante sont rédigées complètement par Saab Abou Jaoudé**

2 La partie rédigée par Saab Abou Jaoudé commence maintenant

Drôle de nom que celui *d'nijection virtuelle*! Les injections virtuelles généralisent les injections naturelles d'un ensemble E dans un ensemble F, qui existent si $card(E) \leq card(F)$, au cas $card(E) > card(F)$. Ce ne sont plus alors des fonctions (et cela serait impossible) mais une relation R sur l'ensemble $E \times F \times F \times E$ des quadruplets (x, y, y', x') définie par la formule $y = y' \Rightarrow x = x'$. En fait, une injection virtuelle est une classe de relations. Lorsque $card(E) \leq card(F)$, la classe est triviale dans un sens que nous allons préciser.

Pour essayer de comprendre ce qui se passe, nous commençons par définir un mode de comparaison des relations binaires, dit comparaison de Tukey, qui nous permet de classifier les relations binaires, puis nous définissons le mode de comparaison des relations "2n-aire", dit comparaison ludique (ou comparaison de Chalons), où n est le cardinal d'un ensemble I d'indices. Nous nous intéresserons ensuite au cas $n = 2$ et $I = \{1, 2\}$ dans lequel figurent les injections virtuelles.

Soit E et F deux ensembles.

Dans tout ce texte nous noterons $E \to F$ l'ensemble des applications de E dans F

3 Ordre de Tukey sur les relations.

Définition 1 (Préordre de Tukey) *Etant donné deux relations (E, F, R) et (E', F', R'), on dira que (E, F, R) est moins puissante (au sens de Tukey) que (E', F', R') et on notera $(E, F, R) \leq_T (E', F', R')$ s'il existe $(f, g) \in (E \to E') \times (F' \to F)$, appelé couple témoin, tel que :*

$$\forall (x, y') \in E \times F',\ (f(x), y') \in R' \Rightarrow (x, g(y')) \in R$$

Proposition 1 *La relation $\leq_T$ est une relation de préordre c'est-à-dire reflexive et transitive.*

Démonstration : Pour obtenir $(E, F, R) \leq_T (E, F, R)$ (reflexivité) il suffit de vérifier que le couple (Id_E, Id_F) est un couple témoin adéquat.
On suppose $(E, F, R) \leq_T (E', F', R')$ de couple témoin (f, g) et $(E', F', R') \leq_T (E'', F'', R'')$ de couple témoin (f', g'). Alors le couple $(f' \circ f, g \circ g')$ est un couple témoin pour $(E, F, R) \leq_T (E'', F'', R'')$ (facile à vérifier), ce qui établit la transitivité de $\leq_T$.

On peut donc poser la définition suivante :

Définition 2 (Degré de Tukey) *La relation $\backsimeq_T$ définie par*

$$((E, F, R) \leq_T (E', F', R')) \text{ et } ((\mathrm{E}', \mathrm{F}', \mathrm{R}') \leq_{\mathrm{T}} (\mathrm{E}, \mathrm{F}, \mathrm{R}))$$

est une relation d'équivalence (réflexive, symétrique et transitive). Les classes d'équivalence sont appelées degrés de Tukey. La relation $\leq_T$ induit sur les degrés de Tukey une relation d'ordre appelé ordre de Tukey. On la note $\leq_T$ par abus de langage.

4 Ordre ludique.

Soit I un ensemble d'indices fixé, et soit (E_i, F_i, E'_i, F'_i) une famille de quadruplets d'ensembles, **tous non vides**, indexés par I. On note $G = \prod_{i \in I} (E_i \times F_i)$ et $G' = \prod_{i \in I} (E'_i \times F'_i)$. On abrégera, pour ne pas alourdir les écritures, les notations $(x_i)_{i \in I}$ et $\prod_{i \in I} X_i$ en (x_i) et $\prod X_i$, sous-entendant l'indexation par $i \in I$.

On considère $R \subset G$ et $R' \subset G'$.

Définition 3 (Comparaison ludique) *On dira que la relation R est ludiquement inférieure à la relation R', et on notera $R \leq_L R'$, s'il existe (pour tout $i \in I$) $f_i : E_i \to E'_i$, $g_i : (E_i \times F'_i) \to F_i$, appelés fonctions témoins, telles que :*

$$\forall (x_i) \in \prod E_i, \forall (y'_i) \in \prod F'_i, (f_i(x_i), y'_i) \in R' \Rightarrow (x_i, g_i(x_i, y'_i)) \in R$$

Comme ci-dessus, il est assez facile de voir, en produisant les fonctions témoins, que la relation $\leq_L$ est une relation de préordre. La relation d'équivalence qui lui est associée définit les degrés ludiques comme classe d'équivalence et l'ordre induit par la relation $\leq_L$ sur les degrés ludiques s'appelle l'ordre ludique qu'on notera $\leq_L$.

La définition ci-dessus montre à l'évidence que les degrés ludiques possédent, pour l'ordre ludique, un plus petit élément appelé *bottom* qui est la classe de la relation pleine ($R = G$), toujours vrai et un plus grand élément appelé

top qui est la classe de la relation vide ($R' = \emptyset$), toujours fausse. On dira que la relation R est *bottom* (resp. *top*) si elle est dans la classe *bottom* (resp. *top*).

On conserve les notations ci-dessus.

Définition 4 (Relation triviale) *On dit que la relation R est triviale s'il existe des fonctions $h_i : E_i \to F_i$ telles que :*

$$\forall (x_i) \in \prod E_i,\ (x_i, h_i(x_i)) \in R.$$

On dira que les fonctions (h_i) sont trivialisantes pour R.

Théorème 1 *Toute relation triviale est bottom.*

Démonstration : Soit (h_i) des fonctions trivialisantes pour R. Il suffit de démontrer que $R \leq_L R'$, avec $G' = \prod(E_i \times E_i)$ et $R' = G'$. On définit $f_i = Id_{E_i}$ et $g_i(x_i, y_i') = h_i(x_i)$. (f_i, g_i) sont, de par le choix des (h_i), des fonctions témoins pour $R \leq_L R'$.

Dans tout ce qui suit, on fixe $I = \{1, 2\}$

5 Injection virtuelle.

5.1 Définition et propriétés élémentaires

On considère deux entiers n et p non nuls en temps qu'ordinaux finis. On a donc $n = \{0, 1, ..., n-1\}$ et $p = \{0, 1, ..., p-1\}$.

On suppose que $(E_1, F_1, E_2, F_2) = (n, p, p, n)$ donc $G = (n \times p) \times (p \times n)$ et on définit

$$R = \{(x_1, y_1, x_2, y_2) \in G \mid y_1 = x_2 \Rightarrow x_1 = y_2\}.$$

Définition 5 *La relation R définie ci-dessus est appelé injection virtuelle de n dans p. On la note $injvirt(n, p)$, ou, plus simplement dans ce texte (n, p).*

Remarque : La définition ci-dessus est une commodité de langage. les ensembles E_1, F_1, E_2, F_2 peuvent être des ensembles de cardinal respectif n, p, p, n, avec la réserve $E_2 = F_1$ et $F_2 = E_1$. Elle se transporte de façon évidente en $injvirt(n, p)$. Nous prendrons indifféremment dans la suite l'une ou l'autre des deux définitions.

Nous allons nous intéresser à la comparaison de deux injections virtuelles (n, p) et (n', p'). Notons d'abord le résultat suivant qui justifie en quelque sorte le nom qui a été donné à cette relation.

Proposition 2 *On suppose que $n \leq p$. Alors (n, p) est triviale.*

Démonstration : Rappelons que $(x_1, y_1, x_2, y_2) \in R \Leftrightarrow (x_1 = y_2)$ *ou* $(y_1 \neq x_2)$.
Soit ϕ une injection de n dans p et ψ une inverse à gauche de ϕ. Soit $a = (x_1, \phi(x_1), x_2, \psi(x_2))$ un élément du graphe de (ϕ, ψ). Alors, ou bien $x_2 \neq \phi(x_1)$ et $a \in R$, ou bien $x_2 = \phi(x_1)$, mais alors $\psi(x_2) = \psi \circ \phi(x_1) = x_1$ et $a \in R$. Nous avons ainsi démontré que le graphe de (ϕ, ψ) est dans R, ce qui établit que R est triviale.

Nous obtenons donc le résultat suivant, valable pour tout couple (n, p) de cardinaux, finis ou non : Si $n \leq p$, alors (n, p) est *bottom.*

Dans la suite on supposera toujours que $n > p$

5.2 Comparaison ludique, démontage logique

Pour étudier la possible comparaison ludique de deux injections virtuelles, nous allons reprendre la définition d'une telle comparaison et la transformer pour la rendre plus utilisable.

Soit $R = (n, p)$, $R' = (n', p')$ deux injections virtuelles non triviales telles que $R \leq_L R'$ et soit $(f_1, f_2, g_1, g_2) \in (n \to n', p \to p', n \times p' \to p, p \times n' \to n)$ un quadruplet témoin. On a le premier résultat suivant :

Théorème 2 *La fonction f_2 est surjective.*

Démonstration : Supposons f_2 non surjective, et soit $y_1' \in p' - Imf_2$. Alors pour tout$(x_1, x_2, y_2') \in n \times p \times n'$, $f_2(x_2) \neq y_1'$, donc $(f_1(x_1), f_2(x_2), y_1', y_2') \in R'$.
D'autre part, pour $y \in n'$, l'application $\phi_y : x \to g_2(x, y)$ va de p dans n. Comme $p < n$, elle n'est pas surjective. On définit ainsi une application $h : n' \to n$ par le choix de $h(y) \notin Im\phi_y$.
On choisit $y_2' \in n'$, $x_1 = h(y_2')$ et $x_2 = g_1(x_1, y_1')$. Le quadruplet (x_1, x_2, y_1', y_2') ainsi choisi réalise $x_2 = g_1(x_1, y_1')$ et $x_1 \neq g_2(x_2, y_2')$, i.e. $(x_1, x_2, g_1(x_1, y_1'), g_2(x_2, y_2')) \notin R$. Nous avons donc démontré que f_2 non surjective implique la négation de $R \leq_L R'$, CQFD.

Pour faciliter les écritures, on va renommer provisoirement (f_1, f_2, g_1, g_2) en (f, h, g, k) et (x_1, x_2, y'_1, y'_2) en $(x, z, y', t') \in n \times p \times p' \times n'$.

On note $A(x_1, x_2, y'_1, y'_2) = A(x, z, y', t')$ l'énoncé

$$(h(z) = y' \Rightarrow f(x) = t') \Rightarrow (z = g(x, y') \Rightarrow x = k(z, t')).$$

Alors,

$$(n, p) \leq_L (n', p') \Leftrightarrow \forall (x, z, y', t') \in n \times p \times p' \times n', A(x, z, y', t').$$

Par contraposition, $A(x, z, y', t')$ est équivalent à :

$$(z = g(x, y') \text{ et } \mathrm{x} \neq \mathrm{k(z, t')}) \Rightarrow (\mathrm{h(z) = y'} \text{ et } \mathrm{f(x) \neq t'})$$

Par élimination de z c'est encore :

$$x \neq k(g(x, y'), t') \Rightarrow (t' \neq f(x) \text{ et } \mathrm{y' = h(g(x, y'))}),$$

ce qui s'écrit encore :

$$(t' \neq f(x) \text{ et } \mathrm{y' = h(g(x, y'))}) \text{ ou } \mathrm{x = k(g(x, y'), t')},$$

soit, par distributivité du "ou" par rapport au "et" :

$$(t' \neq f(x) \text{ ou } \mathrm{x = k(g(x, y'), t')}) \text{ et } (\mathrm{y' = h(g(x, y'))} \text{ ou } \mathrm{x = k(g(x, y'), t')}).$$

En définitive, si $(n, p) \leq_L (n', p')$, cela veut dire qu'il existe un quadruplet témoin

$$(f, h, g, k) \in (n \to n') \times (p \to p') \times (n \times p' \to p) \times (p \times n' \to n)$$

tel que, pour tout $(x, y', t') \in n \times p' \times n'$, on a :

$$x = k(g(x, y'), f(x)) \text{ et } (\mathrm{y' = h(g(x, y'))} \text{ ou } \mathrm{x = k(g(x, y'), t')})$$

Ces relations nous suggèrent de considérer les deux applications suivantes :

$$u : \left\{ \begin{array}{c} n \times p' \to p \times n' \\ (x, y') \to (z = g(x, y'),\ t' = f(x)) \end{array} \right. ,$$

et :

$$v : \left\{ \begin{array}{c} p \times n' \to n \times p' \\ (z, t') \to (x = k(z, t'),\ y' = h(z)) \end{array} \right. .$$

Calculons $v \circ u$. On a :

$$v \circ u(x, y') = v\,(g(x, y'), f(x)) = (k(g(x, y'), f(x)), h(g(x, y'))) = (x, h(g(x, y')))\,,$$

avec $h(g(x, y')) = y'$ si (x, y') vérifie la condition : l'application $t' \to k(g(x, y'), t')$ est non constante.

5.3 Une condition nécessaire.

Cela nous conduit à considérer l'ensemble B des $z \in Im(g)$ tel que l'application $t' \to k(z, t')$ est constante et l'ensemble A des $x \in n$ tel qu'il existe $y' \in p'$ vérifiant $g(x, y') \in B$. En symbole :

$$\begin{array}{rcl} B & = & \{z \in Im(g) \mid \exists x \in n : \forall t' \in n',\ k(z, t') = x\} \\ A & = & \{x \in n \mid \exists y' \in p' : g(x, y') \in B\} \end{array}$$

La définition de B nous permet d'associer, à tout $z \in B$, l'ensemble non vide B_z des x témoins de $z \in B$. On a :

Lemme 1 *Pour tout $z \in B$, B_z est un singleton et $A = \bigcup_{z \in B} B_z$.*

Démonstration : Soit en effet $z = g(a, b) = g(c, d) \in B$. On a

$$c = k\,(g(c, d), f(c)) = k\,(z, f(a)) = k\,(g(a, b), f(a)) = a$$

L'égalité $A = \bigcup_{z \in B} B_z$ est une conséquence immédiate de la définition de A.

Il en résulte une surjection de B sur A. Notons r le cardinal de A et s le cardinal de B. On a $r \leq s$. Notons que $s \leq p$ puisque $B \subset p$. Nous sommes en mesure de démontrer :

Théorème 3 *Avec les mêmes notations, si $(n,p) \leq_L (n',p')$ alors il existe un entier naturel $r \leq p$ tel que*

$$(n-r)p' \leq (p-r)n'$$

Démonstration : Avec les notations qui précédent, soit $x \in n-A$. Par définition de A, quelque soit $y' \in p'$, $g(x,y') \notin B$. La restriction de l'application u à $(n-A)\times p'$ prend ses valeurs dans $(p-B)\times n'$ et cette restriction, inversible à gauche, est injective. On en déduit puisque $r \leq s$:

$$(n-r)p' \leq (p-s)n' \leq (p-r)n'$$

c'est-à-dire le résultat annoncé.

En fait on a un résultat plus général concernant $g^{-1}(z),\ z \in p$:

Lemme 2 *Soit (x_1,y'_1), (x_2,y'_2) deux éléments de $n\times p'$ tels que $g(x_1,y'_1) = g(x_2,y'_2) = z \in p$. On suppose que $x_1 \neq x_2$, alors $y'_1 = y'_2$ et $f(x_1) \neq f(x_2)$*

Démonstration : On a, en tout état de cause :

$$k\left(g(x_1,y'_1),f(x_1)\right) = x_1 \ \text{ et } \ \mathrm{k}\left(\mathrm{g}(\mathrm{x}_2,\mathrm{y}'_2),\mathrm{f}(\mathrm{x}_2)\right) = \mathrm{x}_2 \neq \mathrm{x}_1.$$

La fonction $t \to g(z,t)$ est ainsi non constante, donc

$$h(z) = h\left(g(x_1,y'_1)\right) = y'_1 \ \text{ et } \ \mathrm{h}(\mathrm{z}) = \mathrm{h}\left(\mathrm{g}(\mathrm{x}_2,\mathrm{y}'_2)\right) = \mathrm{y}'_2.$$

On en déduit que $y'_1 = y'_2$.
La relation $f(x_1) \neq f(x_2)$ est alors évidente puisque

$$k(z,f(x_1)) = x_1 \neq x_2 = k(z,f(x_2)).$$

On en déduit immédiatement :

Théorème 4 *Pour tout $z \in p$,*

1. *Soit il existe $x \in n : g^{-1}(z) \subset \{x\}\times p'$.*
   On dira que z est de type L (contenu dans une ligne)
2. *Soit il existe $y' \in p' : g^{-1}(z) \subset n \times \{y'\}$.*
   On dira que z est de type C (contenu dans une colonne).

De plus, lorsque z est de type C, la restriction de f à la première coordonnée de $g^{-1}(z)$ est injective. Le cardinal d'un tel $g^{-1}(z)$ est donc $\leq n'$.

Définition 6 (Ensemble-ligne, ensemble-colonne)
1. *On appelle ensemble-ligne toute partie de $n\times p'$ de la forme $g^{-1}(z)$ où z est de type L.*
2. *On appelle ensemble-colonne toute partie de $n\times p'$ de la forme $g^{-1}(z)$ où z est de type C.*

On se permettra de parler de lignes dans l'ensemble $n\times p'$. Ce sont les sous-ensembles de la forme $\{x\}\times p'$. De même, on parlera de colonnes, ensembles de la forme $n\times\{y'\}$.

Vue ce qui précède, un ensemble-colonne est contenu dans une colonne et son cardinal est $\leq n'$. Un ensemble-ligne est contenu dans une ligne et son cardinal est bien évidemment $\leq p'$. Ces remarques nous serviront dans la sous-section 5.5

Notons l le nombre de z de type L, c le nombre de z de type C. Les $g^{-1}(z)$ formant une partition de $n\times p'$, on a :

$$np' \leq lp' + cn' \ \text{ avec } \ \mathrm{l}+\mathrm{c} = \mathrm{p}$$

5.4 Quelques exemples

Nous reprenons, dans ce qui suit les notations (f_1,f_2,g_1,g_2) et (x_1,x_2,y'_1,y'_2). La formulation équivalente de $(n,p) \leq_L (n',p')$ devient :
il existe un quadruplet témoin

$$(f_1,f_2,g_1,g_2) \in (n\to n')\times(p\to p')\times(n\times p'\to p)\times(p\times n'\to n)$$

tel que, pour tout $(x_1,y'_1,y'_2) \in n\times p'\times n'$, on a :

$$x_1 = g_2(g_1(x_1,y'_1),f_1(x_1)) \ \text{ et } \ (\ \mathrm{y}'_1 = \mathrm{f}_2(\mathrm{g}_1(\mathrm{x}_1,\mathrm{y}'_1)) \text{ ou } \mathrm{x}_1 = \mathrm{g}_2(\mathrm{g}_1(\mathrm{x}_1,\mathrm{y}'_1),\mathrm{y}'_2))$$

Nous supposerons que l'on a toujours à faire à des injections virtuelles (n,p) non triviales, ce qui implique $n > p$.
Voici les premières paires simples d'injections virtuelles pour lesquelles il est facile de décider :

Théorème 5 *Soit n, p, n', p' quatre entiers naturels non nuls tels que $p < n$, $p' < n'$*

1. *On suppose $p < p'$. Alors la relation $(n,p) \leq_L (n',p')$ est* ***fausse.***
2. *On suppose $n > n'$ et $p = p'$. Alors la relation $(n,p) \leq_L (n',p')$ est* ***fausse.***
3. *Par contre, si $n < n'$ et $p = p'$, alors $(n,p) \leq_L (n',p')$.*
4. *si $n = n'$ et $p > p'$, alors $(n,p) \leq_L (n',p')$*

Démonstration : Notons $R = (n,p)$, $R' = (n',p')$. On suppose $R \leq_L R'$ et soit

$$(f_1, f_2, g_1, g_2) \in (n \to n', p \to p', n \times p' \to p, p \times n' \to n)$$

un quadruplet de fonctions témoins. On va utiliser les théorèmes 2 et 3 pour établir (1) et (2). Pour (3) et (4), on exhibera un tel quadruplet témoin.

1. Supposons $p < p'$. Alors $f_2 \in p \to p'$ ne peut être surjective. On termine par application du théorème 2.
2. Supposons $n > n'$ et $p = p'$. Par utilisation du théorème 3 supposons l'existence d'un $r > 0$ tel que $(n-r)p \leq (p-r)n'$. On en déduit $r(n'-p) \leq p(n'-n)$, donc $r < 0$ et la condition nécessaire pour avoir $(n,p) \leq_L (n',p')$ n'est pas satisfaite.
3. Supposons $n < n'$ et $p = p'$. On prend pour f_1 l'injection canonique de n dans n', pour f_2 l'identité de p. On définit g_1 par $g_1(q,r) = r$. On note h une inverse à gauche de f_1 et on définit g_2 par $g_2(q,r) = h(r)$. Soit (q_1, q_2, r'_1, r'_2) tels que $f_2(q_2) = q_2 = r'_1$. Ceci implique $f_1(q_1) = q_1 = r'_2$. Le cas $f_2(q_2) \neq r'_1$ étant trivial, nous avons démontré que (f_1, f_2, g_1, g_2) est bien un quadruplet témoin.
4. Supposons $n = n'$ et $p > p'$. La démonstration est presque comme ci-dessus, avec une injection ϕ de p' dans p, f_1 l'identité de n, f_2 une inverse à gauche de ϕ, g_1 et g_2 ayant des définitions évidentes.

Voici deux autres injections virtuelles comparables :

Proposition 3 *On a :* $\forall (n,p) \in \mathbf{N}^{*2}, n > p \Rightarrow (n+1, p+1) \leq_L (n,p)$

Démonstration : Rappelons que $n+1 = \{0, 1, 2, ..., n-1, n\}$. On définit :
- $f_1(x) = x$, si $x < n$ et $f_1(n) = 0$
- $f_2(x) = x$, si $x < p$ et $f_2(p) = 0$
- $g_1(x, y') = y'$ si $x < n$ et $g_1(n, y') = p$
- $g_2(x, y') = y'$ si $x < p$ et $g_2(p, y') = n$

Il est fastidieux de vérifier que (f_1, f_2, g_1, g_2) est un quadruplet témoin car il faut faire une énumération de cas. Nous laissons donc cette vérification au bon soin du lecteur.

On en déduit facilement que pour tout r entier naturel, on a

$$(n+r, p+r) \leq_L (n,p)$$

Voici une autre paire d'injections virtuelles comparables.

Proposition 4 *On a :* $\forall (k,n,p) \in \mathbf{N}^{*3}$, $(kn, kp) \leq_L (n,p)$

Démonstration : On suppose évidemment que $n > p$.
Soit K un ensemble de cardinal k, N un ensemble de cardinal n et P un ensemble de cardinal p. On prend $E_1 = K \times N$, $F_1 = K \times P$, $E_2 = N$, $F_2 = P$ et on construit les fonctions témoins

$$(f_1, f_2, g_1, g_2) \in (K \times N \to N) \times (K \times P \to P) \times ((K \times N) \times P \to K \times P) \times ((K \times P) \times N \to K \times N)$$

- $f_1((a,b)) = b$.
- $f_2((c,d)) = d$.
- $g_1((a,b), e) = (a, e)$.
- $g_2((c,d), f) = (c, f)$.

Il suffit de faire le calcul automatique de la condition équivalente rappelée au début du paragraphe pour terminer la démonstration.

Encore une paire :

Proposition 5 *soit $0 < p' < p < n < n'$ des entiers naturels. On a :* $(n,p) \leq_L (n',p')$

Démonstration : On dispose d'une injection de n dans n' qui sera f_1. On note h un inverse à gauche de f_1. On dispose d'une injection k de p' dans p dont un inverse à gauche sera f_2. On définit $g_1(x, y') = k(y')$ et $g_2(x, y') = h(y')$. On a bien un quadruplet témoin.

Une fois ces exercices de vérifications fait, on peut examiner, en cas d'existence d'un quadruplet témoin de $(n,p) \leq_L (n',p')$, qu'est-ce que cela implique sur les entiers n,p,n',p' dans le cas où

$$p > p' \quad \text{et} \quad \mathrm{n} > \mathrm{n}',$$

les autres cas ayant déjà été traités. Allons d'abord chercher une condition suffisante, en utilisant les résultats précédents.

Soit q et r le quotient et le reste de la division euclidienne de p par p' i.e. $p = qp' + r$ et $0 \leq r < p'$. Avec ces notations on obtient en appliquant les résultats ci-dessus :

$$(n,p) \leq_L (n-r, p-r) = (n-r, qp').$$

Dans ces conditions, si $n - r \leq qn'$, alors :

$$(n-r, qp') \leq_L (qn', qp') \leq_L (n',p').$$

Nous avons ainsi établi le théorème :

Théorème 6 (condition suffisante) *Soit (n,p,n',p') quatre entiers naturels, q et r le quotient et le reste de la division euclidienne de p par p'. Alors :*

$$n \leq qn' + r \Rightarrow (n,p) \leq_L (n',p').$$

Pour démontrer que cette condition est nécessaire, il nous suffit d'établir que la relation $(kn+1, kp) \leq (n,p)$ est fausse, ce qui est une conséquence immédiate du théorème 3. Non, pas tout à fait. Si le "r" fourni par théorème 3 est plus petit que le "r" fourni par le théorème précédent, la condition nécessaire n'est plus suffisante. Par exemple $(65,18) \leq_L (20,5)$ est faux alors que $(65-1).5 = 320 \leq 340 = (18-1).20$.

Il est donc nécessaire d'aller plus loin que la considération de la partie A mise en évidence avant le lemme 1. Le théorème 4 de structure va nous permettre de faire ce pas.

5.5 Nécessité de la condition du théorème 6

Supposons donc que $(n,p) \leq_L (n',p')$. Le théorème 4 nous a permis de mettre en évidence deux entiers naturels (l,c) tels que

$$l + c = p \ \text{ et } \ \mathrm{np}' \leq \mathrm{lp}' + \mathrm{cn}' = \mathrm{l}(\mathrm{p}' - \mathrm{n}') + \mathrm{pn}'.$$

Ecrivons la division euclidienne de p par p' : $p = qp' + r$.

Nous allons démontrer que la condition $n > qn' + r$ est contradictoire.

Supposons donc $n > qn' + r$. On a alors :

$$(qn' + r)p' < np' \leq l(p' - n') + (qp' + r)n',$$

soit, après transformation :

$$0 < (r - l)(n' - p')$$

Comme $n' > p'$, il en résulte que $l < r$. On en déduit que $n - l > qn'$. Il faut donc au moins $q+1$ ensemble-colonnes (voir définition 6) pour recouvrir la partie d'une colonne de $n \times p'$ non couverte par les ensemble-lignes. Comme il y a p' colonnes, il en résulte que $c \geq (q+1)p'$, donc :

$$p = l + c \geq l + qp' + p' > qp' + r = p,$$

ce qui est contradictoire. D'où le théorème :

Théorème 7 *Soit (n,p,n',p') quatre entiers naturels tels que $n > p$, $n' > p'$. Soit q et r le quotient et le reste de la division euclidienne de p par p'. Alors, une condition nécessaire et suffisante pour avoir*

$$(n,p) \leq_L (n',p')$$

est

$$n \leq qn' + r$$

6 La preuve initiale d'Anatole Khélif

On suppose $n' \geq p'$ et $(n,p) \leq (n',p')$ et on note f,g,h,k les fonctions témoins. Soit $A := \{x \mid \forall y \exists t : x \neq k(g(x,y),t)\}$ et remarque que $\phi : (x,y) \mapsto (g(x,y),f(y))$ est une injection de $A \times p'$ dans $p \times n'$ puisque étant donné (x,y) dans $A \times p'$, on a $x = k(g(x,y),f(x))$ et $y = h(g(x,y))$.

La fonction f va de n dans n' et en particulier, sa restriction à A va de A dans n'. Posant $a := card(A); k := [a/n']$, il existe $v \in n'$ tel que v a au moins k antécédents $x_1, \ldots x_k$ dans A par f. L'injectivité de ϕ fournit alors que $B := \{g(x_i,y) \mid i \in \{1;\ldots k\}; y \in p'\}$ est tel que $card(B) = k \times p' = [a/n'] \times p'$.

Pour $x \notin A$, il existe $y(x)$ tel que $\forall t : k(g(x,y(x)),t) = x =: m(g(x,y(x)))$. Or si $x' \in A$ il n'est pas possible que $x \notin A$ et $g(x,y(x)) = g(x',y')$. En effet, sinon $x = k(g(x,y(x)),f(x')) = k(g(x',y'),f(x')) = x'$ alors que $x \notin A$ et $x' \in A$. L'ensemble $C := \{g(x,y(x)) \mid x \notin A\}$ a un cardinal égal $n - a$ puisque $x \notin A \mapsto m(g(x,y(x))) = x$ est l'identité, donc injective et on vient de voir que $B \cap C = \emptyset$.

Tout ce petit monde habite dans p. Il y a donc au moins $[a/n'] + n - a$ éléments dans p. Rappel : $k := [a/n']$. On a donc $kp' + n \leq p + a \leq p + kn'$. Il s'en suit que $kp' + n \leq p + kn'$ donc $n - kn' \leq p - kp' = (q-k)p' + r \leq (q-k)n' + r = qn' - kn' + r$ donc $n \leq qn' + r$